IJCSC 0973-7391 Volume 8 • Issue 1 Sept 2016 - March 2017 pp. 55-62 available online at www.csjournalss.com

Cloud Computing: A Review

Richa Singla[1], Richa Dutta[2]

[1]M.Tech Student, Yamuna Institute of Engineering & Technology, Gadholi (Yamuna Nagar).

[2]Assistant Professor, Yamuna Institute of Engineering & Technology, Gadholi (Yamuna Nagar).

Abstract: This paper gives a brief review of cloud computing by describing its definition, types, benefits and limitations. This review paper simply uncovers all the security issues and challenges commonly faced in cloud computing. Among all issues, data security and privacy are vey important topics which will have to be certainly address in upcoming years for the growth of cloud computing strategy.

Keywords: Private Cloud, Public Cloud, Hybrid Cloud, Security issues, Benefits of cloud computing.

Introduction

Cloud computing provides the latest technologies and softwares as on demand to the cloud user on pay per use basis. Cloud computing strategy is the extension of the concepts of distributed, utility and grid computing, It provides the computing resources as utility to the organizations similar to other utilities such as electricity, water etc.

For big IT, giant ventures like Google and Microsoft, can easily buy and manage IT infrastructures and their legitimate software's, but comparatively smaller organizations or start-ups can't afford big investments merely in buying IT infrastructures and their legitimate software's because investment size matters to smaller enterprises. Along with the investment, managing these big machines and type of expertise require will cost even more. So, cloud computing offers a resolution of all these investments and management issues for such small organizations. This technology substitutes the actual physical IT infrastructure with the virtual IT infrastructure through the virtualization technology which can be accessed just through an internet connection.

Now the organizations need only concerned about the computing facilities they are seeking for without concerning about their underlying details to provide those services. In cloud user's data is stored into massive data centers and can be accessed from any connected device to the cloud all over the world.

A survey by International Data Corporation (IDC) was conducted among 263 IT giants and their associated business colleagues (as shown in figure 1.1), to collect their sentiments on services offered by cloud computing vendors.

Now as in cloud, all the vital data and applications are stored at cloud vendor site, it has increased a great data security and privacy concern of the cloud users (as resulted from IDC survey in figure 1.1). So now the next challenge is to assure cloud users about their data security, integrity and privacy before adopting to the new environment.

So now it is the duty of cloud vendor to assure their customers about the same reliability, privacy and secure control on their applications as they have at their own place.

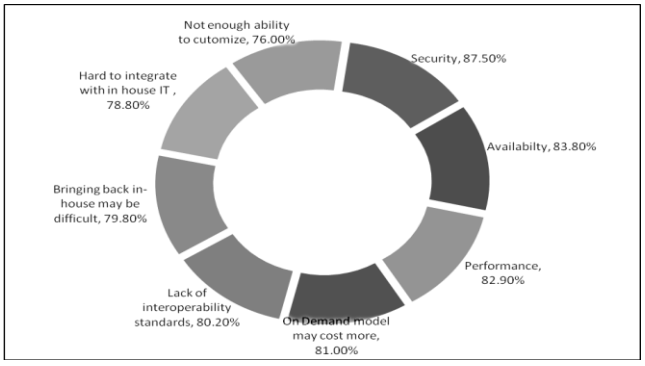

Figure 1.1 - Results of IDC ranking security challenges (n = 263)

1.1 Cloud Computing

There are lot of widely accepted definitions of cloud computing paradigm, some of them are listed as under.

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." - U.S. National Institute of Standards and Technology (NIST). [1]

"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption" - Forrester Research, Inc. [2]

"A style of computing where massively scalable IT-enabled capabilities are delivered as a service to external customers using Internet technologies." - Gartner, Inc. [3]

"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" - R. Buyya, C. S Yeo, and S. Venugopal [4]

Cloud computing is mainly enhancement of the concepts of distributed computing, utility computing and grid computing. The features of all these above concepts are merged to provide the new concept.

1.2 Cloud Computing Models

Cloud computing paradigm propose the renting of both the software and hardware as a service to the end user over the internet through web browser (see Figure 1.2). Cloud computing vendors classify their cloud software and hardware services among three categories [5]:

i. Software as a Service (SaaS)
ii. Platform as a Service (PaaS)
iii. Infrastructure as a Service (IaaS)

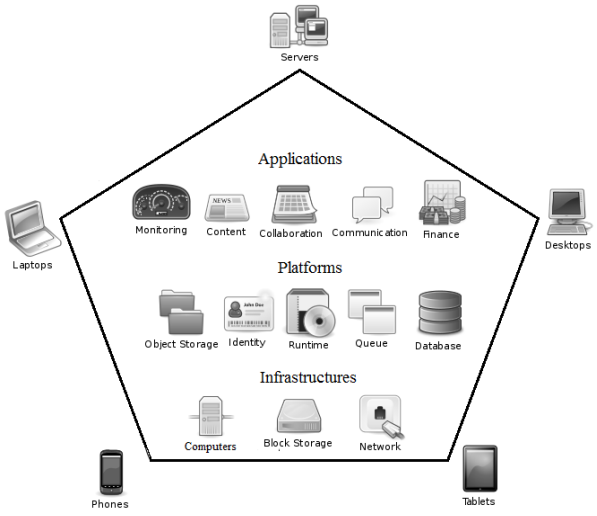

Figure 1.2 - Layers in Cloud Architecture

1.2.1 Software As A Service (SAAS)

Software as a Service [5] is a software delivery model in which cloud vendor delivers software's directly to its client's machine through a web browser and user will be charged on pay per use basis. Now the cloud users will be free from managing the cloud infrastructure and platform running at back end on which his rented application is executing. It also eliminates the requirement of bulky payment for the legitimate software's. Because now he can use the legitimate software's by raising a request to its vendor and the vendor will provide access of the required

software within minimal time. So, the cloud end user need not to concern about the licensing and genuineness of required software.

1.2.2 Platform As A Service (PAAS)

Similar to SaaS cloud delivery concept, it is designed to deliver computing platform as a service through the internet web browser and using it virtually to run the user's applications [5]. Now user can rent any platform environment on their web browser and can develop, deploy and run their programs on the virtual platform provided by the cloud vendor. Now the end user will be mainly concerned about programs on their rented platforms (typically including operating system, databases, execution environment, compilers and web servers etc.) not about the infrastructure in back end. All the tools required during the complete life cycle of development of web applications will be provided by PaaS completely through the internet connection.

1.2.3 Infrastructure As A Service (IAAS)

In this model, the cloud vendors deliver the Infrastructure i.e. equipment's those are required to support all softwares and operations again through the internet connection [5]. The equipment's mainly include storage devices, hardware, servers and various networking components etc. Cloud vendor provide required IT infrastructures such as virtual machines, raw (block) storage, load balancers, firewalls, and networks etc. User use the required resources with his internet connection but they are actually installed in cloud vendor's datacenters. Cloud vendor is fully responsibility for housing, running and maintaining of these IT equipment's. The individual or client organizations need only to pay on per-use basis. It is also known as Hardware as a Service (HaaS).

Figure 1.3 shows the difference in the number of portions of the whole server stack that a customer of an IaaS, PaaS and SaaS provider is responsible to control as compared to a private on-premises server.

Figure 1.4 shows the various cloud computing service models and the services, applications offered by big IT cloud giants in the respective categories.

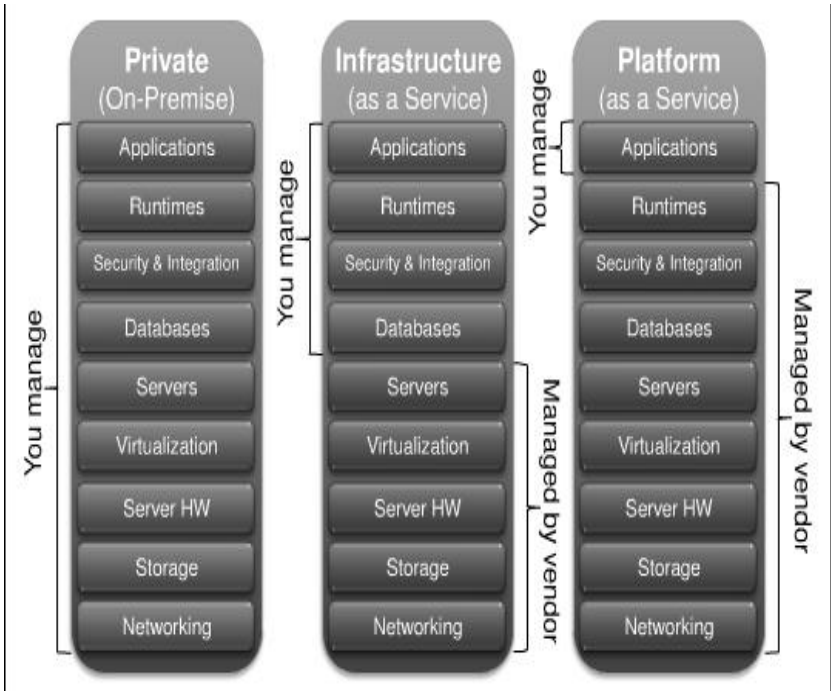

Figure 1.3 - Server stack comparison between Private (on premise), IaaS and PaaS.

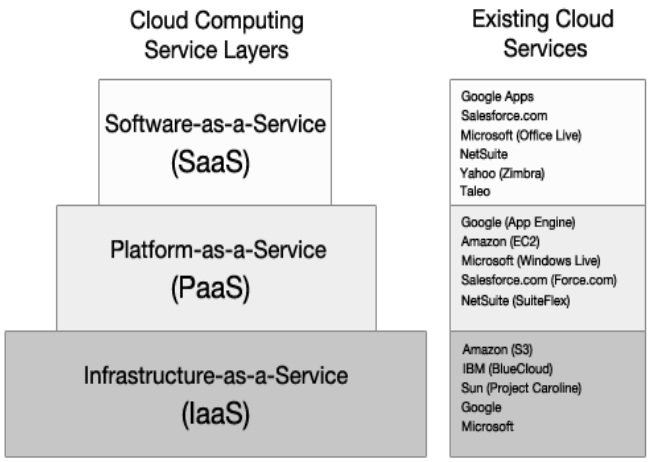

Figure 1.4 - Service Models Applications

1.3 Deployment Models

Today cloud computing is one of the most growing paradigm due to variety of deployment models which satisfies the need of vast range of consumers such as for individual, large industries, startups and many more. On the basis of demand of the users, the different categories of clouds are [6] [13] [16]:

1.3.1 Public Cloud

In this cloud deployment model, the cloud services are used by the general public or the large-scale organization without managing the cloud infrastructures. The cloud vendors are responsible for managing all the cloud services. The end user or the organizations don't have any responsibility of controlling, operating and securing the cloud services as figure 1.5 shows.

Figure 1.5 - Public Cloud

The public cloud is managed by the cloud vendor outside the premises of cloud user, so that the user will be free from every responsibility by just paying pay per use basis. It helps a lot to startups and small organizations by reducing their set-up investments as well as operational expenditures. The cloud services can be scaled up or down as per user demand in no time.

Apart from benefits of public cloud, it suffers with a serious concern. As the user cloud services are maintained outside his premises, so his private and sensitive data will be stored and processed outside his premise, so security and integrity of his data is generally a main concern.

1.3.2 Private Cloud

In this cloud deployment model, the cloud services are used solely by individual organization within its premises [5] [13]. The cloud user can control or maintain the services its own or hire cloud vendor or any third party for the control and management of rented cloud services. So, in this category the cloud user is responsible for managing all

the cloud services inside his firewall. The vendor doesn't have any responsibility of controlling, operating and securing the cloud services as figure 1.6 shows.

Figure 1.6 - Private Cloud

Mainly private cloud is managed by the cloud user enterprise inside his premises, so that the user has more control on his private and sensitive data, which was the main concern of the user in using public cloud.

Apart from benefits of private clouds, it suffers from a major disadvantage of requirement of big set up investment, operational expenditure as well as highly skilled technicians which ultimately increases the startup expenditure of the organization as compared to public cloud.

1.3.3 Hybrid Cloud

This cloud deployment model, is the combination of two or more types of clouds, private or public [6]. So that it combines the benefits of both deployment models. So that now the cloud vendors have developed some integrated solutions of private and public clouds which combine their benefits as shown in figure 1.7.

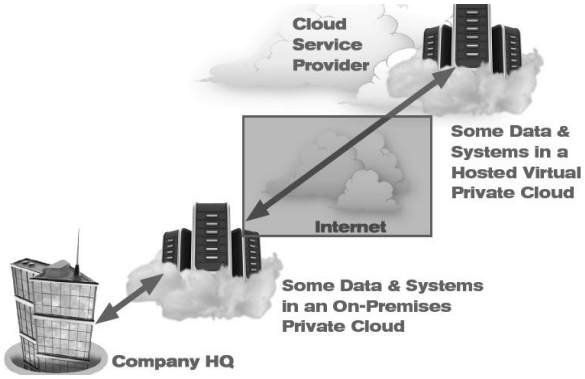

Figure 1.7 - Hybrid cloud

So, in hybrid clouds the private or sensitive data is maintained in the private cloud at user's premise and the non-sensitive data is sent to the public cloud maintained outside his premise. Which increases the user control on his data in the hybrid clouds, hence security and integrity of data will be increased.

1.3.4 Community Clouds

In this deployment model, several users having similar requirements are treated as a community, so that they can share an infrastructure and might share the configuration and management of the cloud. This management might be done by themselves or by third parties.

1.4 Benefits of Cloud Computing

There are lots of benefits of cloud computing paradigm as compared to traditional computing strategies [7]. The cloud computing strategy reduces starting investment, scaling of the resources, eliminate the operational cost, ease of maintenance, reduces risk factors etc. Some of the important benefits are described as under:

1.4.1 Reduced Starting investment and Operational Cost

As utility computing is the idea behind cloud services, so user need only to pay per use basis. So, the starting investments in purchasing big IT infrastructures and in hiring of their maintenance expert team is massively reduced. Now the small organization and individual startups can implement their idea with almost negligible investments with the renting of desired cloud services.

1.4.2 Improved Scalability

Cloud users can effortlessly acquire (scale up) and release (scale down) the required computing resources on demand in the minimal time. So that the cloud users will be free from wastage of the bought resources.

1.4.3 Effective & Improved Resource Utilization

As the past studies shows that only 10 to 20 % of the bought hardware's is really used in its life time. Which results into about 80% wastage of the bought resources throughout its life. But since various cloud resources are shared among many cloud users from a pool of resources. So that overall utilization of shared resources increases up to 80% so that its cost is better utilized by cloud vendor as compared to individual user.

1.4.4 Location and Device Independence

Cloud vendors provide the power of accessing various cloud services just through an internet connection through a web browser. This gives the location independence to the cloud users. Additionally, the cloud services can be accesses on any type of devices such as mainframe computers, personal computers, PDA, mobiles etc. Since accessing of cloud services just require internet connection so it gives the location and device independence to cloud users.

1.4.5 Hassle free Maintenance

As only the big giants can make investment as cloud vendors, so they also hire a team of professional and experts to maintain their cloud resources. The hired team are generally best in their class so that they have more ability to maintain the cloud resources. But cloud users can't afford hiring of such expertise level of professionals and experts. So that the experts at cloud vendor site ensure ease to use, support, maintenance to their clients instantly. This ensures an outstanding service quality to the cloud users.

1.4.6 Multi-Tenancy

Since in cloud computing strategy multiple cloud users share same pool of cloud resources still each user work on its own copy of resources. The cloud user boundaries are isolated on the shared cloud resources.

1.4.7 Improved Reliability

As the expertise, data centers and disaster recovery plans of the cloud vendors are far much superior than the cloud user. So, reliability has greatly improved with the shifting to clouds.

1.4.8 Increased Security

As the expertise of the cloud vendors are far much superior than the cloud user. So, security has greatly increased due to centralization of data and better security strategies.

1.5 Limitations of Cloud Computing

Cloud computing the one of the main buzz word in the IT market. It provides a lot of flexible options to every user. The cloud computing strategy has massively reduced starting investment, ease of scaling of the resources, eliminate the operational cost, ease of maintenance, reduces risk factors etc. some of the cloud vendors have established themselves in the market and some of their cloud based applications, such as Gmail, Facebook etc., have achieved great success; But the main concern of today's user is security and integrity of their off-shore data located in geographically distributed data center of cloud vendors [12].

Now days mainly all cloud users are outsourcing their less sensitive data to the cloud data centers due to lack of trust, security and reliability of the data [8]. As a lots of data thefts has been reported in the past.

1.5.1 Data Security and Confidentiality

As after adopting cloud services, all the data (sensitive or non-sensitive) is stored in cloud vendor data centers. Cloud user uses some of his data frequently and other non-frequently. So generally, data may be in transit or rest. Which create additional challenges for the data in transit [14] [15]. Attackers can explore the vulnerabilities of the internet connection and transmission medium to steal or alter the data. Which may affect the confidentiality and integrity of the cloud user data.

1.5.2 Service Unavailability

As all the data of cloud user is stored at cloud vendor data centers through internet connection. So, delay in the delivery of cloud service, non-availability of internet connection and vulnerabilities in the internet connections may result into a delay in service to the cloud users. Which is not favorable at all for the growth of the cloud services.

1.5.3 Data Lock-In

After using services of any cloud vendor, if cloud user want to some other vendor or to in-house data centers that will be nearly impossible [9]. The various cloud vendors don't use the standard APIs so that the portability and interoperability among them is very limited, which result into a stage of data lock-in with current cloud vendor.

1.5.4 Cross VM attacks

Multi-tenancy is one of the major USP of cloud computing paradigm. In which all the cloud users share same physical machine and storage hard disks. In this several virtual machines are virtualized on the one physical machine by using hypervisors softwares and their access given to the different cloud users. Similarly, various cloud users are co located on the same hard disks.

As two cloud users can share same physical machine, due to which some cross virtual machine attacks have been spotted in past which compromise the machine and storage of the victim user. So, it is a big issue for cloud vendors to isolate the various cloud users from each other.

1.5.5 Insider Attack

As all the cloud user data (sensitive or non-sensitive) is stored at the cloud vendor data centers. Now some of the malicious cloud vendor employee can affect the integrity, privacy and security of the user data. He can steal data of any cloud user and sell it to his competitor which may impact and damage the customer's brand, reputation, or trust.

Because same types of attacks have been identified in the past years, so that the cloud vendor must audit the involvement (defining who can access the data and by what level) of all his every employee regularly to maintain faith of their cloud users.

1.5.6 High Response Time in Scaling Resources

As scaling up and scaling down as per cloud user need is one of the biggest advantages of cloud. But if the response time in fulfilling of demand will be very high then its benefit will be of no use. As well as scaling up must be allowed only up to a threshold level because some malicious cloud user can raise demand for resources unnecessarily to implement Denial of Service attack on the cloud vendor which will in turn increase the response time of other cloud users of same vendor. Thus, the customer could be billed for the service that they did not want.

So, all options must be worked out during service level agreements (SLA) regarding maximum response time allowed.

1.5.7 Data Location

As after adopting cloud services, all the data (sensitive or non-sensitive) is stored in cloud vendor data centers. Cloud user uses some of his data frequently and other non-frequently. So generally, data may be in transit or rest. But the data at rest may be distributed geographically, that is another concern of cloud users in cloud computing. Different countries have different rules and regulations, so if in one country the data may be safe but in another may not. So, the cloud user has full right to choose among the available data centers as well as they have right to know the flow of data among data centers at the time of SLA [10].

Currently some of the vendors like Amazon leave the choice of the datacenter location to the user such as US, Europe etc.

1.5.8 Remittance of the Deleted Data

As soon as some cloud user will delete his data on vendor data center, still some remittance of the data remains on the vendor hard disk. So, through side channel attacks, malicious insider attacks, cross VM attacks etc. can retrieve the deleted data which can be further used for the disgrace of the cloud user's company reputation and

Some latest reports such as by European Network and Information Security Agency (ENISA) [11] has suggested that data at rest must be encrypted so that level of the risk due to recovery of deleted data can be minimized.

1.5.9 Recovery and Back-Up

Cloud vendors store their data at geographically distributed data centers, so the providers should have a data back-up plan in the case of disaster situations. Generally, cloud vendor tackle this issue by having replica of the data at different data centers so that data will be safe always in some data center.

1.6 Conclusion

In the paper, we have justified that it is very important to take security and privacy into account while using and shifting towards cloud services. This paper uncovers all the security issues and challenges commonly faced in cloud computing.

Among all issues, data security and privacy are most important topics which will have to be certainly addressed in the coming years for the success of cloud computing. So that products that will come with the security and shortcoming management concepts in market will stay in high demand in future.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing". National Institute of Standards and Technology, NIST, 2009.

[2] J. Staten. "Is cloud computing ready for the enterprise?" published at Forrester Research, March, 7, 2008.

[3] DC Plummer, TJ Bittman, T. Austin, D. Clearley, and DM Smith, "Cloud computing: Defining and describing and emerging phenomenon" published at Gartner Inc., September 25, 2008.

[4] R. Buyya, C.S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering its services as computing utilities" published in the 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08), pages 5–13, IEEE, 2008.

[5] Minrui Jia, "Cloud Security of Cloud Computing Application" published in International conference on Control, Automation and Systems Engineering (CASE), ISBN: 978-1-4577-0859-6, pp: 1 – 4, July, 2011.

[6] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, "Cloud Computing Security--Trends and Research Directions" published in IEEE World Congress on Services, Washington, DC USA, ISBN: 978-0-7695-4461-8, July 2011.

[7] D. Catteddu and G. Hogben., "Cloud computing: benefits, risks and recommendations for information security" Technical report published by European Network and Information Security Agency, 2009.

[8] Kelton Research. Survey: Cloud Computing "No Hype", but fear of security and control slowing adoption. http://tv.sys-con.com/node/852659.

[9] The Guardian. Cloud computing is a trap, warns GNU founder Richard Stallman. http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman, 2008.

[10] Inc. Forrester Research. Cloud privacy heat map., http://www.forrester.com/cloudprivacyheatmap, 2010.

[11] B. Hay, K. Nance, and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing," published in pproceedings of the 44th Hawaii International Conference on System Sciences pp. 1–7, Jan., 2011

[12] Popovic, Kresimir Hocenski, Zeljko, "Cloud computing security issues and challenges" published in pproceedings of the 33rd International Convention Date: 24-28, pp: 344 – 349, Print ISBN: 978-1-4244-7763-0, July 2010.

[13] Manpreet Kaur, Hardeep Singh, "A review of Cloud computing security issues", published in International Journal of Advances in Engineering & Technology, ISSN: 22311963, Volume-8, Issue-3, pp397-403, 2015.

[14] Amar Nath Bhargava, Neha Bhardwaj, "A Review of Services on Security in Cloud Computing", published in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume: 6, Issue- 5, pp: 799-804, May 2016.

[15] Meikang Qiua, b, Keke Gaib, Bhavani Thuraisinghamc, Lixin Taob, Hui Zhaod,, " Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry", Published in Elsevier, http://doi.org/10.1016/j.future.2016.01.006, 2016.

[16] Karolj Skala, Davor Davidovic, Enis Afgan, Ivan Sovic, Zorislav Sojat, "Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing", published in Open Journal of Cloud Computing (OJCC), DOI: 10.19210/1002.2.1.16, Volume: 2, Issue: 1, Pages 16-24, 2015.